National Cybersecurity Center of Excellence (NCCoE)
Energy Sector

Energy Provider Community of Interest

23 August 2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE Energy Sector News
- Current Projects
    - Identity and Access Management (IdAM) Project Update
    - Situational Awareness (SA) Project Update
- Oil and Natural Gas Sub-sector Development
- Open Discussion

NCCoE Out and About:

- Upcoming planned conferences
  - ICS Cyber Security Conference (Sacramento, 10/3/2016)
  - GridSecCon (Quebec City, 10/17/16)
    - *4 hour workshop planned*
    - *Topics include:*
      - NIST NCCoE overview, including Cyber Security Framework
      - Top challenges in the industry from industry, association, and integrator perspective
      - NCCoE Solutions: applied cybersecurity; that is, example solutions to guide the industry from the NIST NCCoE (i.e. IdAM & Situational Awareness for Electric Utilities; Industrial Control System Security topics including but not limited to Leveraging NCCoE Elec. Utilities Body of Work for Oil and Gas)
  - SGIP Grid Modernization Summit 2016 (Washington, DC, 11/7/2016)

OVERVIEW: IDAM SECTOR CHALLENGES

Challenges we heard from industry:

- **Lack of authentication, authorization, and access control requirements for all OT**
- **Inability to manage and log authentication, authorization, and access control information for all OT using centralized or federated controls**
- **Inability to centrally monitor authorized and unauthorized use of all OT and user accounts**
- **Inability to provision, modify, or revoke access throughout the enterprise (including OT) in a timely manner**

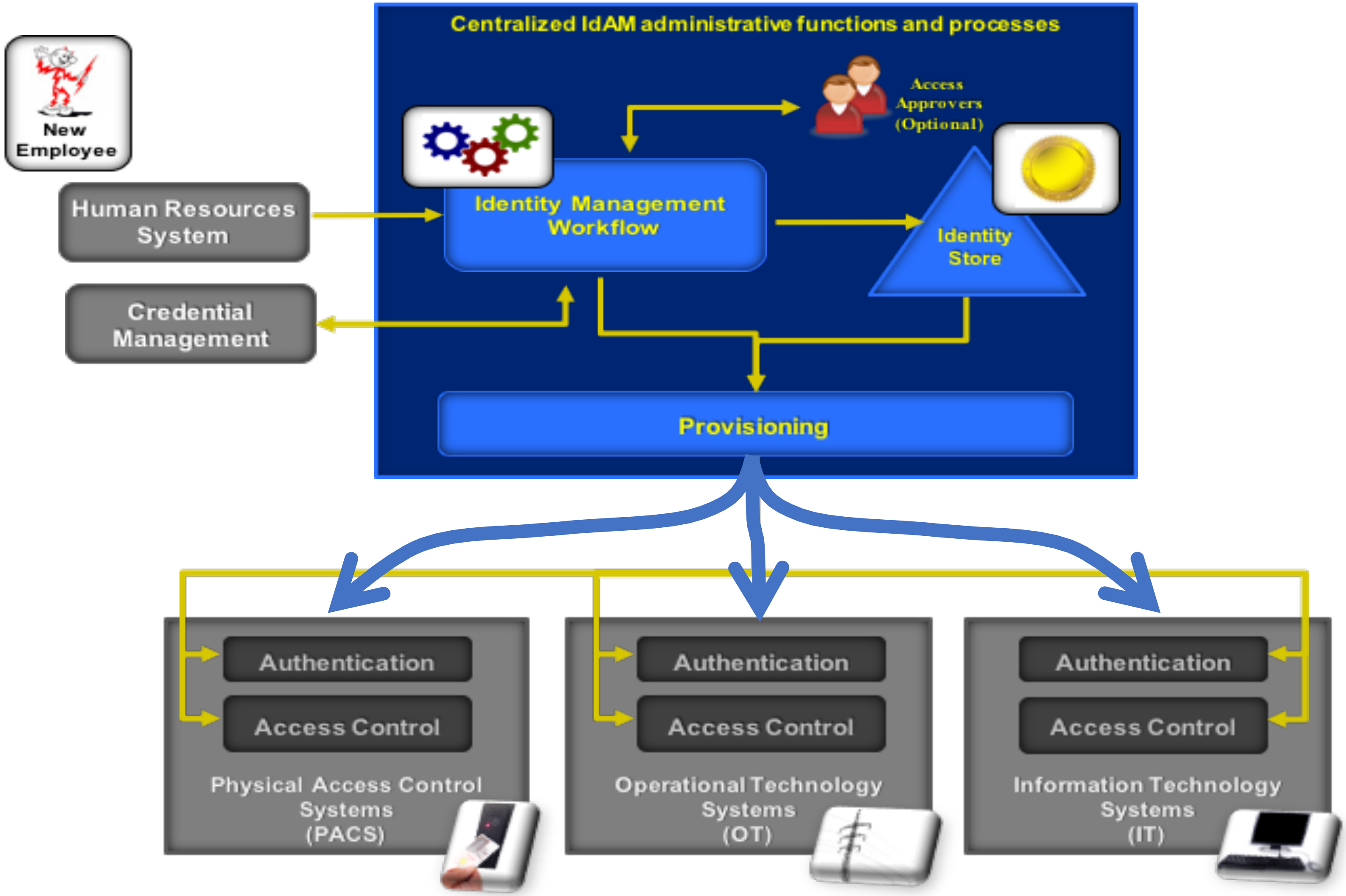
Solution NCCoE built:

- ✓ Authenticates individuals and systems
- ✓ Enforces authorization control policies
- ✓ Unifies IdAM services
- ✓ Protects generation, transmission and distribution
- ✓ Improves awareness and management of visitor accesses
- ✓ Simplifies the reporting process

Converged management of silos

Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam

CURRENT PROJECTS: IDAM SOLUTION


New Employee
Human Resources System
Credential Management
Centralized IdAM administrative functions and processes
Access Approvers (Optional)
Identity Management Workflow
Identity Store
Provisioning
Authentication
Access Control
Physical Access Control Systems (PACS)
Authentication
Access Control
Operational Technology Systems (OT)
Authentication
Access Control
Information Technology Systems (IT)

CPS Energy (San Antonio) and NCCoE are collaborating on a case study to document a worked example, lessons learned, and known benefits. Expect to complete by October.

OVERVIEW : SITUATIONAL AWARENESS SECTOR CHALLENGES

Industry Challenges:

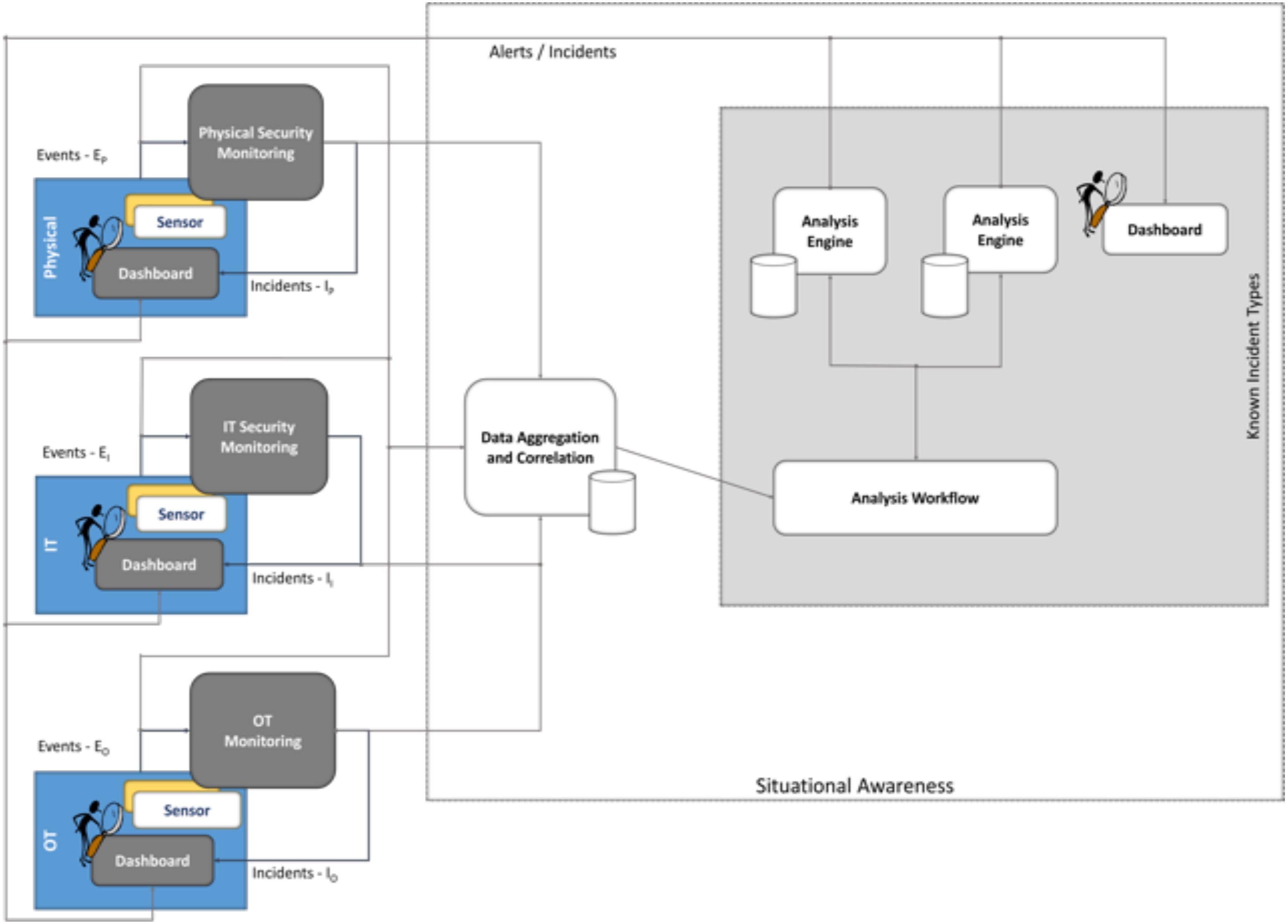
- Improve OT availability
- Detect anomalous conditions and remediation
- Unify visibility across silos
- Investigate events leading to baseline deviations/ anomalies
- Share findings

Solution NCCoE is developing:

- ✓ Improves the ability to detect cyber-related security breaches or anomalous behavior
- ✓ Improves accountability and traceability
- ✓ Simplifies regulatory compliance by automating generation and collection of operational log data
- ✓ Increases the probability that investigations of attacks or anomalous system behavior will reach successful outcomes

Use Case is online at https://nccoe.nist.gov/projects/use_cases/situational_awareness

CURRENT PROJECTS: SITUATIONAL AWARENESS

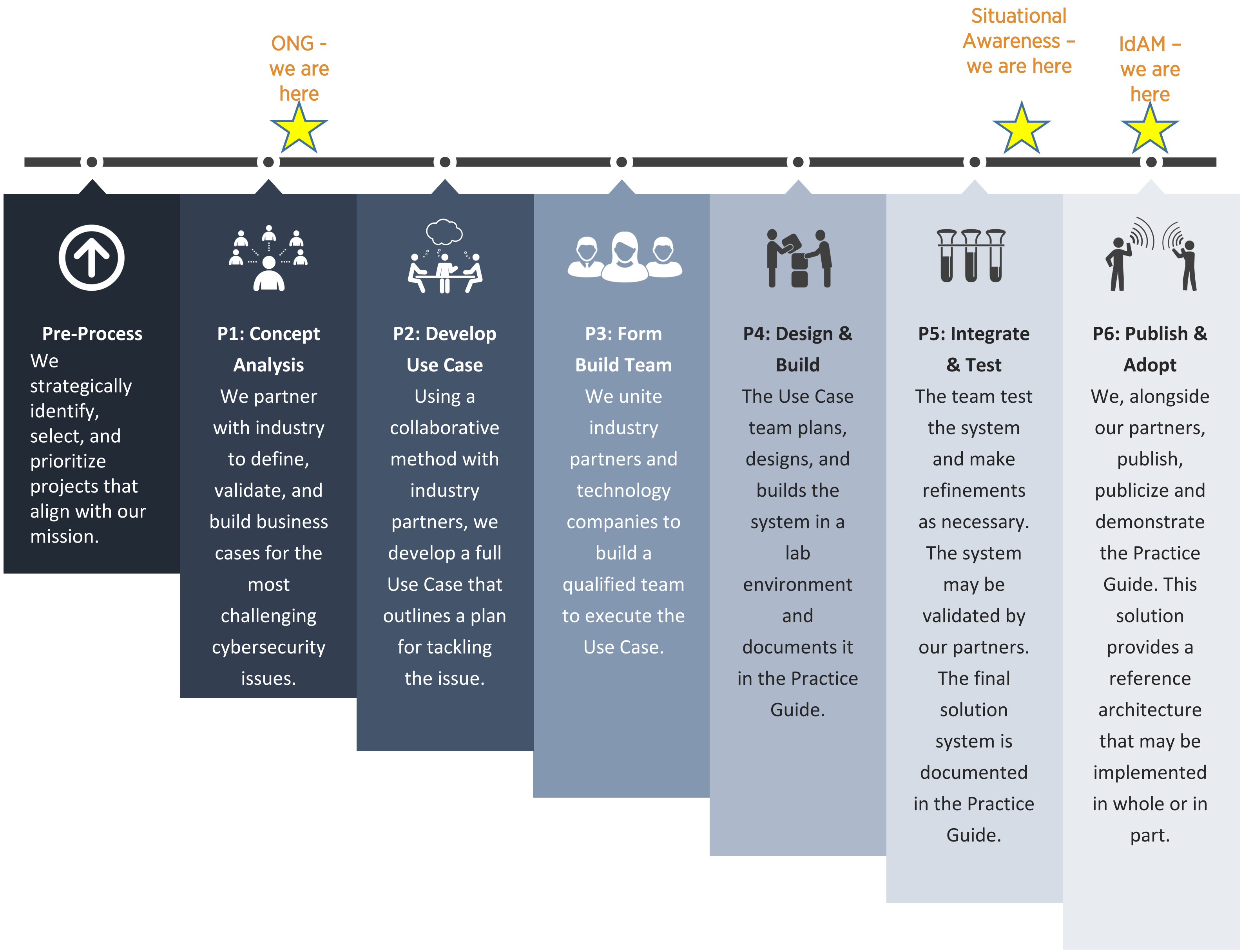


PROJECT MILESTONES

PROJECT NAME: IdAM	Upcoming Milestone Dates
Publish Special Publication	Thu 09/29/16

PROJECT NAME: Situational Awareness	Upcoming Milestone Dates
Completed Build	Wed 08/31/16
Release Draft Practice Guide for Public Comments	Thu 09/29/16
Publish Special Publication	Thu 03/30/17

PROJECT PHASES



ONG - we are here

Situational Awareness – we are here

IdAM – we are here

Pre-Process
We strategically identify, select, and prioritize projects that align with our mission.

P1: Concept Analysis
We partner with industry to define, validate, and build business cases for the most challenging cybersecurity issues.

P2: Develop Use Case
Using a collaborative method with industry partners, we develop a full Use Case that outlines a plan for tackling the issue.

P3: Form Build Team
We unite industry partners and technology companies to build a qualified team to execute the Use Case.

P4: Design & Build
The Use Case team plans, designs, and builds the system in a lab environment and documents it in the Practice Guide.

P5: Integrate & Test
The team test the system and make refinements as necessary. The system may be validated by our partners. The final solution system is documented in the Practice Guide.

P6: Publish & Adopt
We, alongside our partners, publish, publicize and demonstrate the Practice Guide. This solution provides a reference architecture that may be implemented in whole or in part.

Icon Credits (right to left): Talking by Juan Pablo Bravo; Test Tube by Olivier Guin; Collaboration by Krisada; Team by Wilson Joseph; Brainstorm by Jessica Lock; Network by Matthew Hawdon; Arrow by Jamison Wieser; all from the Noun Project.

BUILDING AN NCCOE OIL & NATURAL GAS SUB-SECTOR

EPC SCOPE IS EXPANDING TO ONG

- Industry-driven awareness
  - Communication with industry regarding the Cyber Security Framework and Transportation Sector/ Maritime USCG profile work has demonstrated the need to address ONG-focused challenges
- Strategic engagement
  - Cybersecurity challenges exist across the expanse of the critical infrastructure
  - Opportunity to develop a repeatable model → force multiplier to enhance cybersecurity across many sectors
- Direct application of our mission and goals
  - Provide practical cybersecurity
  - Increase rate of adoption
  - Accelerate effective innovation

INDUSTRY ENGAGEMENTS AND INTERACTION TO DATE (1)

- NCCoE/USCG Cyber Security Profile outreach efforts:
  - Conference attendance:
    - **2015 API Cybersecurity Conference**
    - **2016 NIST CyberSecurity Framework Workshop**
    - **2016 Offshore Technology Conference** and established contacts
  - Industry - large oil companies, offshore drilling companies, pipeline companies, shipping companies
  - Trade Associations:
    - American Petroleum Institute (API) –
      - Cybersecurity Committee
      - Annual Cybersecurity Conference (will speak at 2016 Conference)
    - American Federation of Petrochemical Manufacturers (AFPM)
  - Federal Advisory Committees
    - National Offshore Safety Advisory Committee (NOSAC) of the US Coast Guard
  - NIST Cybersecurity Framework outreach - NCCoE CSF Pre-Conference Workshop
  - ISACs - Director of the ONG ISAC, FS-ISAC, DNG-ISAC
  - Houston InfraGuard program

INDUSTRY ENGAGEMENTS AND INTERACTION TO DATE (2)

- Industry connections and discussions with industry, including
  - FERC
  - Black & Veatch
  - Berkeley Research Group (BRG)
  - Automation Federation
  - ISA
  - Army Corps of Engineers
- Down Stream Natural Gas ISAC engagement with Cybersecurity Threat Analyst specializing in ICS/SCADA systems

TAKEAWAYS FROM ONG ENGAGEMENT TO DATE

- Cybersecurity motivated with complex challenges
  - Many that align with NCCoE mission
  - Some similarities to challenges in other ICS-reliant industries
- Examples of emerging themes
  - Asset inventory and management
  - Supply chain risk management
  - Technology compatibility and interoperability
  - Information sharing (Situational Awareness foundational to this)

PATH FORWARD

- Build a community of interest related to ONG
- Identify critical needs in the sub-sector
- Launch new projects in the sub-sector
    - Gather industry input between now and mid-Sept
    - Share ideas with industry in mid-Sept
    - Submit Needs Assessment(s) to NCCoE leadership for approval (end Sept)

INDUSTRY INPUT

- Your thoughts?

- Open Discussion

CONTACT US

301-975-0200

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850

100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

ABOUT THE NCCOE

FOUNDERS

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®

Department of Business & Economic Development

MONTGOMERY COUNTY
1776
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

TENETS

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector’s individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results